The Information Revolution and Information Security Problems in Russia

By Dr. Vitaliy N.Tsygichko

Editorial Abstract: Dr. Vitaliy Tsygichko states the global community must define "what is an information weapon" and must develop an international convention to limit their use. This should be done under United Nations (UN) auspices in order to prevent the proliferation of information weapons and effectively resist the threats of information warfare, information terrorism, and information crime. Dr. Tsygichko lays out Russia's position on this issue in the form of recommended elements of an international convention.

Introduction

The late 20th and early 21st centuries were marked by the next phase of technological change, notably, the introduction of information and telecommunications technologies (ITT) across nearly all vital activities—and the development of the World Wide Web. Information and telecommunications network technologies and the fast spread of local and global networks provide a new quality of information exchange, shape a new global information space, and impact all facets of public life: politics, economics, culture, international relations, plus national and international security.

Changes in the world information space act as a global development factor, and determine the key directions of social progress. Most important among these are:

- Acceleration of scientific, technological, economic, social, and cultural developments thanks to greater volume and speed of information exchange irrespective of distance.
- Opportunities for dissemination of new ideas and knowledge plus rapid proliferation of scientific and technological achievements.
- Creation of a basis for the elaboration and spread of a new scientific and philosophical paradigm for the 21st century based on understanding the many facets of the world and on the realization of humankind's common global problems.
- Intensification of global integration trends, in particular in economic, political, information, technological, educational, cultural, and other areas.
- Creation of premises for the development and introduction of new forms and methods of ensuring global, regional, and national security.
- Progress in the areas of political, economic, production, military control, and international relations.

Insignia of the Russian Federation Armed Forces. (Wikimedia)

At the same time, the world community's "computerization" breeds a whole set of negative geopolitical implications. First comes polarization of the world (resulting in the widening of the gap between rich and poor and between technologically backward and advanced countries) and the realization of a growing number of marginal countries along the roadside developing civilization. These countries are the main source of instability for current and future conflicts including those of a global character. Thus, the information revolution not only accelerates civilization's progress, but gives rise to new national, regional, and global security threats—primarily terrorism.

The Information Revolution in Military Affairs

New IT changes are most radical in the military. Recent developments clearly point to the fact that military power still remains the key argument behind global and regional policies. Moreover, the significance of military force keeps increasing. After the Cold War the world entered a period of regional wars and political instability as the number of large-scale military operations of a global, regional, and national character increased sharply. Attempts to curb nuclear proliferation failed. Under these circumstances, the US—the recognized leader of the Western world—and their allies set out to cope with these security challenges and defend their national and group interests by establishing and maintaining a "new world order" based largely on threatening the direct use of military force. This US implements this strategy primarily by building up military power, through reorganization of the armed forces in line with the tasks and supply issues associated with a new generation of arms. All of these make wide use of new information technologies. Desert Storm operations, actions in the former Yugoslavia, and the current war in Iraq, illustrate this strategy in practice.

The wide introduction of new information technologies greatly increases combat capabilities of conventional arms and defense-related technologies. Information technologies foster qualitative changes in reconnaissance and communication, producing manifold increases in the speed of processing huge arrays of information that decision-makers require. This permits the transition to new methods of troop and weapons control at all levels—from strategic to tactical. New information technologies made it possible to sharply increase the combat capabilities of electronic warfare equipment and to develop a radically new type of armament: information weapons designed for destroying the defense and civilian information infrastructure of likely enemy threats, by breaking into their computer networks.

While resulting in dramatic increases in combat capabilities of troops, the military ITT revolution leads not only to changes in the forms and methods of conducting operations, but also alters the traditional armed struggle paradigm. Emergence of information weapons has drastically changed the pattern of escalation for military conflicts. Even selective utilization of information weapons against defense and civilian information infrastructure projects can put an end to a conflict in its early phase—before the start of active combat operations. Possession of information weapons, just as with nuclear ones, secures an overwhelming military advantage over countries who have none. In the near future, information and political parameters of "soft power" will dominate the older nuclear ones—if they are not already doing so today.

Realistically, we can refer to the consequences of applying wide-scale military information-technologies and information weapons as a new type of weapon of mass destruction—with all the ensuing realities and problems. The vulnerability of all countries to information weapons, in particular the highly developed ones, is particularly notable. Like nuclear weapons, the latter can serve both as a factor of political pressure and containment.

Clearly information warfare is not a virtual reality game, but rather a quite tangible tool for gaining victory in a military or political conflict. There is no doubt that information weapons are a major component of the military potential of a nation. Many countries, primarily the US and China, are persistently and actively preparing for the conduct of information warfare. The paradox is while a serious military conflict between developed nations is unlikely today, modern weaponry appears hardly effective against the global threat of international terrorism. The latter makes wide use of information technologies—the Internet in particular—for its own ends.

Terrorism and the Civilization Factor

The developed countries' preparedness to rebuff international terrorism is due largely to the civilization factor, which is gaining in significance along with the evolution of civil society. As a complex, multifaceted, and extremely negative socio-political phenomenon, terrorist activities have long since crossed national boundaries, turning into a huge threat to the security of all humanity.

It is a mistake to assume terrorism is composed of separate acts committed by loners or individual terrorist organizations. Clearly, Islamic extremists draw their followers from among the countries preaching Islam. Numerous fundamentalist organizations, quite active in virtually all countries, are recruiting their adherents from among young people. As a rule, these organizations are under the secret patronage of a number of states, and a significant segment of the population in the Arab world sympathizes with their activities. Islamic fundamentalist movements are generously financed and guided by highly influential and rich radical layers in the Muslim world. The extremist propaganda machine is quite efficient at putting ideas in the heads of Muslims of the necessity of Islam's confrontation with the rest of the world, and the inevitability of a war between the two civilizations. Apparently, the Western world will have to wage a protracted ideological struggle for the Muslim mind, as well as economic and military fights over liquidation of sources of terrorism, and creation of economic and socio-political conditions where terrorist threats are minimized.

Extremists chose terrorism as their main and rather effective weapon for war with an unprepared world. The 11 September events in the United States exposed a considerable vulnerability of Western civilization, even to isolated terrorist acts. Political and socio-economic transformations over the past two decades have led to a sharp increase in—and frequently to a dominance of—the "civilization factor" in the developed democracies' perceptions. Chief among these are the purposes, conditions, forms, and consequences of military force utilization.

The civilization factor is defined as an attitude toward the value of human life established in each concrete community (state, religious, or ethnic). This attitude is determined by historical, cultural, and religious traditions; living standards; form of political system; the dominating ideology in each state; the level of development of democracy; and democratic institutions in each society. For example, in Afghanistan under the Taliban regime, human life was of no value—while in Western countries human beings are treated as a basic value of society, and all government institutions are called upon to defend them.

In advanced democratic nations, strengthening of the civilization factor is linked primarily with evolution of civil society as the key socio-political force bearing upon domestic and foreign policy. These include defense, and exercising public control of authorities. The core value in civil society is human life—the rights and security of the individual. Though the process of civil society's formation is ambiguous and frequently controversial, it would be safe to say that it tends to deepen and spread across an ever-wider range of countries in a persistent and irreversible manner. The military way of handling foreign policy problems is unacceptable for civil society if combat operations may result in considerable losses of both one's own citizens, and the enemy's civilian citizens. Of course, this holds only for those situations not threatening the state's existence. In case of aggression against them, battle casualty attitudes

The Russian Federation. (Univ. of Texas)

will be quite different, when they will no doubt make sacrifices for the sake of retaining their sovereignty and independence. But the current geopolitical situation is such that these nations/alliances dominate the world in economic, political, and military respects, and they are facing no direct military threat. Today's terrorist threat is quite real, and the West may accept certain sacrifices while fighting it. As civil society gets entrenched, it becomes more difficult to use military force in situations not threatening the state's existence. So, as far as advanced democratic nations are concerned, it is the civilization factor—the level of admissible casualties in handling foreign policy problems by military means—that is attaining ever-larger significance. In recent decades, experience gained in military conflicts of a different scale in reveals the level of admissible losses amounts today to only scores of human lives. This becomes one of the major factors restraining these nations from use of military force.

This factor manifested itself most fully in the still smoldering Balkans crisis. Military-political implications of the former Yugoslavia conflict made it necessary to radically revise many strategic assessments linked to the use of force in local conflicts. Notably, NATO operations in Yugoslavia deadlocked in mid-May 1999, with the alliance on the brink of a split over two key issues: continuation of bombing; and the possibility of a land operation. NATO air operations failed to produce the desired results, and the Yugoslav army retained most of its combat capability. It was prepared to put up heavy resistance against NATO use of land forces in case of a ground invasion. Aerial bombing—carefully targeted as it may be—inevitably resulted in civilian casualties which sharply undermined the operational support of European public opinion. In fact, Greece was against the military operation, and the Italian and German governments faced problems within their respective parliaments. Even under threat of the alliance's disintegration, public humiliation, and in effect, revision of the outcome of the Cold War, NATO was unprepared for a ground operation. Such is the influence of the civilization factor. Though within the boundaries of the European "province," NATO operations demonstrated the impossibility of realizing military power, even in a small military conflict.

The civilization factor is also behind the deadlock in Iraq, which is experiencing a civil war with no prospects for an end in sight, despite the presence of a big foreign contingent and attempts to regenerate the Iraqi Army. Deaths of Western alliance soldiers and Iraqi civilians keep mounting, reaching a level where public opinions in Coalition countries are more and more persistently urging to pull their units out of Iraq. This in spite of the fact it may lead to yet another victory of Islamic radicals over the civilized world, and to a further escalation of their activities in other regions, including Russia.

In the rest of the world, outside the club of developed nations, the civilization factor does not yet play a significant role. Regional military conflicts of a different scale and character do not generally take the value of human life into consideration. The 1980s Iran-Iraq war, practically all wars in Africa, the civil war in Afghanistan, the China-Vietnam conflict, the armed struggle of Kurds for independence from Turkey, —and other military conflicts associated with the huge loss of human life—are all examples.

Disregard for human life is specifically characteristic of Islamic extremism, where principles of self-sacrifice in the struggle with "infidels" provide terrorists with huge advantages in their war against Western civilization. The latter is incapable—by its very nature—of sacrificing its citizens, and answer terror with terror. Effective counterterrorism is possible only through joint efforts on a global scale. The entire world community must coordinate its anti-terrorist activities, to include those in the area of information terrorism.

Information Terrorism

As an integral part of technological terrorism, the spread of information or cybernetic terrorism poses a serious global threat. Though this type of criminal activity is not yet a widespread, practical terrorist activity, there is a rather high near term danger. Terrorists make use of the civilized world's openness for attaining their ends. In the past, it was more difficult to arrange and execute terrorist acts because of the associated distance and the coordination difficulties. Today, the Internet has practically erased both of these problems. New "network terrorists" are increasingly coordinating doctrinal, conceptual, and organizational level activities using the latest technological advances.

Characteristic features of information terrorism are "cheapness," and difficulty of detection. By linking computer networks across the globe, the Internet has altered the rules concerning sophisticated weapons. Internet anonymity allows a terrorist to become invisible—and practically invulnerable—in the course of his or her criminal action.

New age high-tech terrorism is capable of causing a systemic crisis for the entire globe, at least in the countries boasting a developed information infrastructure. Terrorists will target computers and special computer-based systems (banking, exchange, archive, research, management, and communication facilities)from TV and communication satellites to radio-telephones and pagers. Electronic mass media facilities such as information agencies and services, computerized radio and TV centers, and publishing complexes are especially attractive for terrorists.

Extremists exploit many network features: relative low cost and accessibility; opportunities for secret development; accumulation, and introduction; and extraterritoriality and anonymity. All of these factors enable uncontrolled proliferation of information weapons, especially if they fall into the hands of aggressive or extremist regimes.

Need for an International Information Security Legal Regime

The emergence of information weapons places the information security problem on a par with other global problems such as nuclear, chemical, and bacteriological weapons proliferation; international terrorism; and drug trafficking. All of these problems are of a global character and none are amenable to solution by one or even several countries.

Thanks to Russian initiatives at the UN, the world community is fully aware of the national and global threats of information war, information terrorism, and information crime. Russia is prepared to adopt practical steps towards their neutralization. Countries sometimes take rather tough measures when countering information security threats, but these are often ineffective due to the anonymous, trans-border nature of the violators. No country is safe fighting information threats on their own. Only installation of an international information security regime, plus the concerted efforts of its participants, can prevent the proliferation of information weapons—and effectively resist information warfare, information terrorism, and information criminal threats.

Russian Federation leadership monitors the strategic picture. (MOD Russia)

Yet the practical steps towards an information security legal regime run into specific problems, making it nearly impossible to draw on past experiences to create regimes capable of banning or limiting weapons of mass destruction. The intrinsic properties of information weapons and their utilization make this problematic.

Firstly, negotiations on international information security issues are hindered by the vagueness and ambiguity of both the subject and object of negotiations. The negotiation subject—ensuring information security—and negotiation objects (information weapons, information warfare, information terrorism, information crimes, and the like) are interpreted differently in different countries. Hence, elaboration of a uniform, universally acceptable frame of reference is the first extremely important step.

The main problem lies in defining the term "information weapons" and developing principles for their identification. What means of armed struggle use information weapons? What are the distinctive features of information weapons? What reasonable arguments can serve as a basis for the definition and classification of information weapons? There are still no satisfactory answers. No uniform basic terminology for holding constructive negotiations on international information security is possible without these answers.

There are two main approaches to defining the term "information weapons." The first treats the capability of some traditional (kinetic) means of destruction to affect military and civilian information infrastructure as the key attribute of information weapons. Following this logic, any type of arms—including conventional means of destruction—can be referred to as information weapons if they are capable of damaging information infrastructure components. This is also the main shortcoming of such an approach. Indeed, it makes no difference in the final count if the municipal services control system was disabled by a program code-based weapon, a powerful electronic pulse, or a direct hit from a conventional bomb.

The second approach suggests all means of destruction and armaments making use of information and telecommunications technologies (ITT) be termed information weapons. But virtually all sophisticated weapons systems employ ITT, and it would be impossible to finely discriminate between information weapons and the entire arms arsenal on the basis of this characteristic.

Some groups attempted to combine the two approaches, such as the suggestion to call means of information infrastructure destruction which use ITT "information weapons." However, such combined approaches fail to alleviate uncertainties in identifying information weapons.

According to these approaches, only software designed exclusively for disrupting information infrastructure (viruses, etc.) can be unconditionally called information weapons. All other modern means of armed struggle incorporating ITT are multi-purpose, designed not only for destroying information infrastructure but also for other combat missions. These means differ from past generation weapons given their higher selectivity and accuracy. They are in a sense "humane" weapons, and are not classified as weapons of mass destruction.

Countries possessing sophisticated weapons, reconnaissance, communication, navigation, and control based on the wide-scale application of ITT, have a decisive military advantage. Naturally, such countries will never become parties to any agreements limiting this advantage. The current US stance clearly illustrates this thesis; this nation bluntly refuses to negotiate on issues associated with information weapons, and resists such discussions in the UN Disarmament Commission. The US is only prepared to consider information terrorism and information crime-related issues.

However, Russia would like to know if it is possible to develop criteria for identification of information weapons (apart from software) that are acceptable to all negotiating parties. Could information security problem criteria only limit multi-purpose weapon systems used against civilian information infrastructure projects, instead of banning them? This raises the question of whether the very issue of banning or limiting manufacture, proliferation, and use of information weapons is feasible at all.

Such negotiations may largely concern only single-purpose weapons designed for affecting the information infrastructure components (weapons based on program codes such as different types of viruses and their means of delivery). However, the universality, secrecy, surprise application, possible wide-scale trans-border utilization, efficiency, and high effectiveness not only make such weapons an extremely dangerous means of destruction, but may significantly hamper installation of a relevant international control system. Further, the overwhelming majority of modern ITT—usable for military, terrorist, and criminal ends—are developed in civilian sectors, hence control of their development and proliferation is highly difficult.

At the same time, the threat of information weapons is real for us all, especially developed nations where the complex information infrastructure supports all vital activities. We are witnessing a situation where only concerted international community efforts can lower the threat. Today, identifying and agreeing on a list of key critical information systems (both public and private), whose functions are critically important for ensuring vital activities plus international security, is a necessity. Identification of this class of information systems will make it possible to develop more effective protection measures, including the right to take retaliatory measures. This will also permit elaboration of international emergency threat response mechanisms, as an IW attack will likely affect the national security of various countries.

Real steps toward pooling global information security efforts would seem to be found through international elaboration and endorsement of a convention (treaty) providing the following:

- Renunciation of information warfare and the development and use of information weapons designed for the destruction of the information infrastructure, including arms based on programmed codes
- Harmonization of national laws governing information security counteractions;
- Elaboration of legal, organizational, economic, military, technological, and other international measures, plus mechanisms for resolving conflicts in the information security area, to counter information warfare, information terrorism, and information crime;
- Development of mechanisms for parties-to-convention interaction in collectively countering information security threats. This would involve the permanent exchange of situation reviews, information on potential adversaries, and emergencies associated with information infrastructures, all with a view to designing adequate countermeasures;
- Compiling a list of critically important national information infrastructure projects, whose destruction may lead to large-scale man-made disasters and casualties;
- International laws for protection of critical information infrastructure projects, with attacks on them considered as a crime against humanity;
- Development of convention-related international control and information security monitoring systems;
- Accountability of convention violators.

In order to prevent a single country or group of countries from unfair or advantageous use of the convention provisions, it would be reasonable to adopt declarations to refrain from:

- Actions leading to dominance and control within information space;
- Denying access to the most sophisticated information technologies, (to counter technological dependence in computerization that could lead to the detriment of other states).

Such declarations would dispel doubts in developing countries as to the non-discriminatory nature of the convention.

The first step toward elaboration and adoption of such an international information security convention could be the establishment—within the framework of the UN—of an international team of experts to analyze the following:

- Scientific elaboration of an agreed frame of reference, including fundamental notions such as "information warfare," "information terrorism," "information crime," "information weapons," etc.;

• Compilation of a list of threats to information security, their classification, and how an adversary might implement them;

• Development of information weapon classification principles and identification criteria;

• Compilation of a list of critical information infrastructure projects, and a description of possible effects of their disruption;

• Compilation of a list of possible information security countermeasures;

• Key principles for the development and functioning of an international system of ensuring information security;

• Compilation of voluntary obligations assumed by convention signatories, and possible measures to be taken against convention violators.

The first of these international teams of experts could develop a method for ensuring international information security, which would determine subsequent team efforts, and serve as a basis for the main provisions of an information security convention.

The concept of ensuring international information security should cover:

• A common perception of information security problems;

• Uniform terminology and a frame of reference;

• An evaluation of the current information security situation;

• An assessment of current and potential threats to information security

• The international community's goals and objectives with respect to ensuring information security;

• A description of problems associated with shaping an international information security legal control regime;

• Measures for countering information security threats;

• Potential information security interaction mechanisms;

• Recommendations regarding developmental principles and key provisions for an international information security convention.

Conclusion

International elaboration of an information security convention could become an important practical step in dealing with the complex information weapons issues. Creation of an international legal regime could go a long way in governing the development, proliferation, and use of information weapons; preventing information wars; and ensuring an effective counteraction to information terrorism and information crimes.